PGP® Integration Guide

November 2006

PGP® Support Package for BlackBerry®
BlackBerry Enterprise Server™
PGP Universal™ Server 2.5
PGP® Desktop Email 9.5.1

Version 4.0

Table of Contents

INTRODUCTION 4

Managed versus Unmanaged Users 4

Bound versus Unbound Users 4

Topology 5

Architecture & Setup Requirements 5

Version Requirements 6

PGP Key Conditioning 6

Transactions 7

Policy Considerations 8

BLACKBERRY ENTERPRISE SERVER SETUP 9

Default Policy Attributes 9

Editing IT Policies 10

Enable BlackBerry Enterprise Server Secure Email Support 11

Pushing Policy to the Handheld 12

Enforcing Policy to Multiple Recipients 12

HANDHELD SETUP 13

Setup 13

KEY GENERATION & HANDHELD IMPORT 16

Unmanaged Users 16

Managed Users 19

MANAGING PUBLIC KEYS 22

Importing a Public Key via Email 22

Importing a Public Key via a Keyserver 22

Importing a Public Key from a Handheld 23

Trusting a Public Key 23

SENDING & RECEIVING EMAIL 24

Sending Email 24

Replying to a Message 25

Receiving Email 25

KEY MANAGEMENT 27

Modifying the Key Store Password Timeout 27

Specifying Keyservers 28

Locating & Saving Ad-Hoc Keys 29

Updating Keys in the Key Store 29

PGP Global Directory 29

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

APPENDIX A: TROUBLESHOOTING 30

SERVER-BASED TROUBLESHOOTING 30

HANDHELD-BASED TROUBLESHOOTING 33

APPENDIX B: MANUAL KEY CONDITIONING 36

SKM KEY CONDITIONING 36

PGP UNIVERSAL SERVER: SKM EXPORT 37

PGP DESKTOP EMAIL: SKM IMPORT 38

PGP DESKTOP EMAIL: REMOVE PREFERRED KEYSERVER 38

REMOVE BZIP2 COMPRESSION 40

REMOVE UNSUPPORTED CIPHERS & REMOVE KEY EXPIRATION 41

PGP DESKTOP EMAIL: EXPORT KEYS 41

PGP UNIVERSAL SERVER: DELETE & IMPORT KEYS 42

GKM AND SCKM KEY CONDITIONING 45

APPENDIX C: AUTOMATED KEY CONDITIONING 46

TROUBLESHOOTING 47

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Introduction

The PGP Support Package for BlackBerry enables end-to-end PGP-encrypted email delivery to or from a wireless BlackBerry handheld. This guide illustrates the installation and configuration requirements of four software components:

Component	Installed on	Notes / Purpose
BlackBerry Enterprise Server	Corporate production PC-based server	**Required**. Must be installed before using this guide. Manages sending and receiving email to handheld users. Optionally proxies policy and key lookups to PGP Universal Server.
PGP Universal Server	Dedicated PC	**Optional**. Must be installed before using this guide. Manages keys for users; establishes and enforces policy for handheld users.
PGP Support Package for BlackBerry	BlackBerry handheld loaded via BlackBerry Desktop Manager	**Required**. Enables handheld-based PGP functions such as key lookup, sending and receiving encrypted and/or signed email.
PGP Desktop Email	User's PC or Mac	**Required**. Processes encrypted email on the user's desktop. Used to condition keys to work in concert with the PGP Support Package for BlackBerry. Can also create the keypair used by the handheld.

Managed versus Unmanaged Users

PGP Universal Server can be used to control outbound email policy. Users in this configuration are known as "managed" users. For example, managed users may or may not be allowed to send plaintext email. Users not under the control of PGP Universal Server are called "unmanaged" users. See "Policy Considerations" on page 8 for more details. Unmanaged users should skip all steps related to PGP Universal Server.

Bound versus Unbound Users

PGP Desktop Email software may be purchased as stand-alone software or may be generated from, and bound to, a particular PGP Universal Server. Stand-alone copies of PGP Desktop Email are "unbound" to a particular PGP Universal Server.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Topology

The components and general topology described by this guide are shown in Figure 1. A state diagram outlining the progress of a secure message sent from a managed BlackBerry handheld to a PGP-enabled desktop is shown in Figure 2 on page 7. The section entitled “Enforcing Policy to Multiple Recipients” on page 12 describes the implications of putting PGP Universal Server into various topologies.

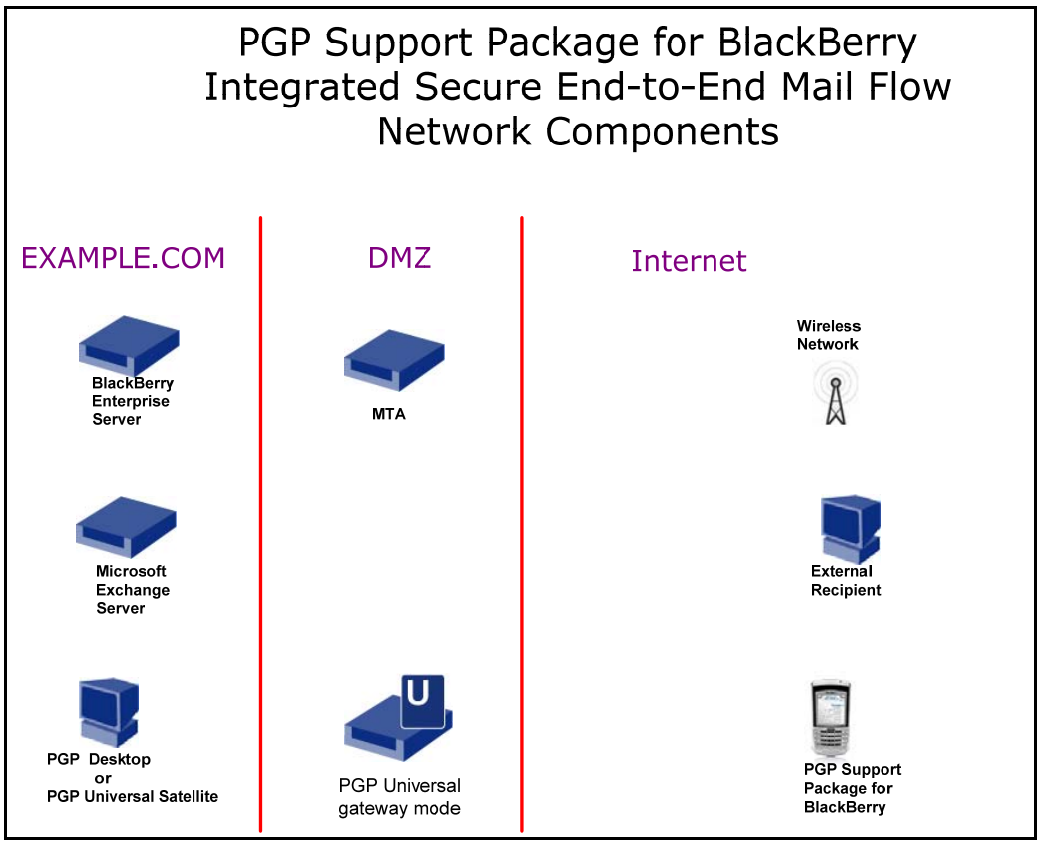


Figure 1: PGP-RIM Topology

Architecture & Setup Requirements

All desktops associated with BlackBerry handheld PGP users must be running PGP software on the desktop. The desktop software options are PGP Desktop Email and PGP Universal Satellite. Users without PGP software can receive messages decrypted by PGP Universal Server operating in gateway mode, but decryption will occur on PGP Universal Server rather than on the desktop. Also, BlackBerry handheld users not running PGP software on the desktop will not be able to read encrypted mail deposited into their Exchange-based “Sent Items” folder.

If deployed, PGP Universal Server should be installed before the PGP Support Package for BlackBerry is installed on BlackBerry handhelds. There are many viable network configuration options, depending on the needs of the enterprise.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

PGP Universal Server should be placed in the DMZ. At a minimum, PGP Universal Server will be used for policy and key lookup. However, there is a compelling reason for placing PGP Universal Server into the mail flow, either directly or on a conditional basis, as described below.

Version Requirements

This configuration requires the following minimum components.

- Optional: PGP Universal Server 2.5
- PGP key requirements (see Appendix B “Key Conditioning”, beginning on page 36, for details)
    - Twofish & IDEA ciphers are disabled
    - Bzip2 compression is disabled (default)
    - PGP-supported ciphers
        - AES (128-, 192-, and 256-bit)
        - CAST (128-bit)
        - TripleDES
- RIM requirements
    - BlackBerry Enterprise Server 4.1.2 or greater
    - BlackBerry Handheld Software 4.2 or greater
    - PGP Support Package for BlackBerry
- Desktop requirements
    - PGP Desktop Email 9.5 or greater or PGP Universal Satellite
    - BlackBerry Desktop Manager 4.0 or greater

PGP Key Conditioning

PGP keys must be “conditioned” to successfully receive email on a handheld device. SKM keys for managed users can be conditioned in bulk as described in Appendix B, beginning on page 36. A tool to condition CKM and GKM keys is described in Appendix C, beginning on page 46. If the tool is inapplicable, manual key conditioning is described beginning on page 19. Condition all keys for all handheld users before continuing with this installation.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Transactions

Figure 2 details the transactions associated with the transmission of a message sent from a PGP-enabled handheld to a PGP-managed desktop inside the same enterprise. The BlackBerry Enterprise Server proxies requests to PGP Universal Server on behalf of the handheld and finally inserts the message into the user's Exchange mailbox.

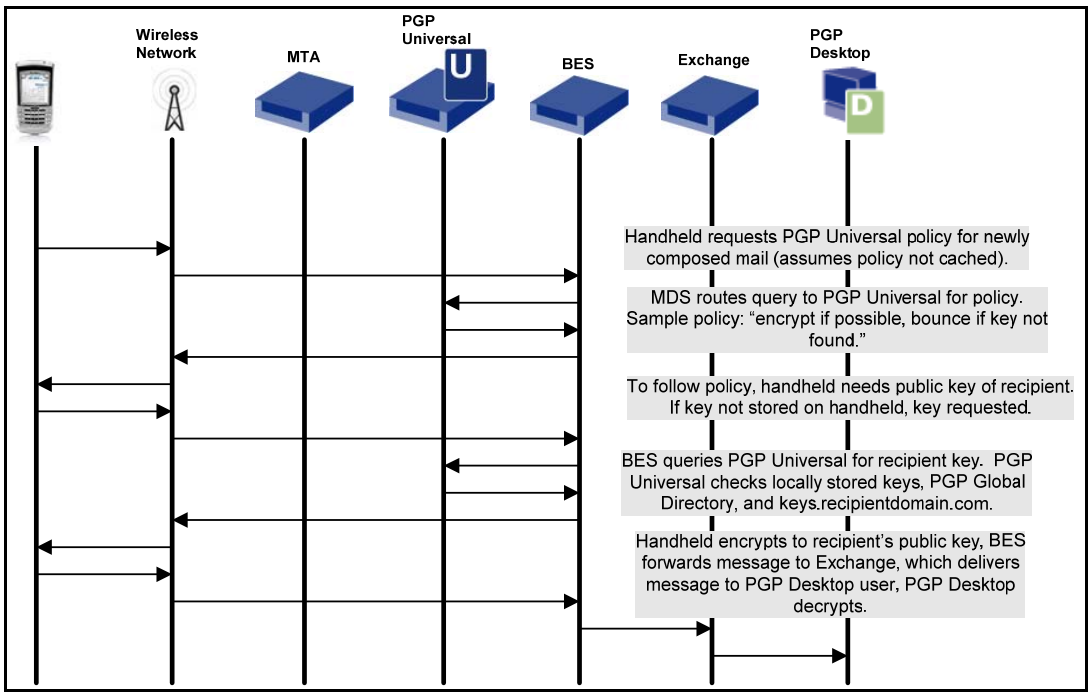

Wireless Network
MTA
PGP Universal
BES
Exchange
PGP Desktop
Handheld requests PGP Universal policy for newly composed mail (assumes policy not cached).
MDS routes query to PGP Universal for policy. Sample policy: "encrypt if possible, bounce if key not found."
To follow policy, handheld needs public key of recipient. If key not stored on handheld, key requested.
BES queries PGP Universal for recipient key. PGP Universal checks locally stored keys, PGP Global Directory, and keys.recipientdomain.com.
Handheld encrypts to recipient's public key, BES forwards message to Exchange, which delivers message to PGP Desktop user, PGP Desktop decrypts.

Figure 2: Message Flow – Managed BlackBerry Handheld to PGP Desktop Email

Considerations:

- The message is never sent or received by the externally facing mail transfer agent (MTA).
- BlackBerry Enterprise Server requests to the BlackBerry infrastructure are stateful outbound TCP-based requests to port 3101 of the BlackBerry infrastructure.
- In this example, the recipient was an internal user, so the public key was found on the local PGP Universal Server.
- The flow of this message to an external domain would be very similar to the transactions shown in Figure 2. However, in the final step, the message would be passed from the Exchange server to the externally facing MTA for delivery to the recipient domain.
- For unmanaged users, policy is defined on the BlackBerry Enterprise Server and the handheld.

Log entries demonstrating the PGP Universal Server processing of a secure message sent from a BlackBerry handheld are shown in the "Troubleshooting" section in Appendix A, beginning on page 30.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Policy Considerations

Both PGP Universal Server and the BlackBerry Enterprise Server permit the administrator to define policy. For managed users, PGP Universal Server enforces compliance from an email security perspective while the BlackBerry Enterprise Server controls the operation of the handheld connected to it. As such, the policies are considered to be separate entities. There may be some overlap in the policy items available to administrators. In all cases, when using a handheld, BlackBerry Enterprise Server IT policy will be enforced before PGP Universal Server policy is applied.

A managed user whose BlackBerry handheld is enrolled with PGP Universal Server cannot send a message that violates PGP Universal Server policy. Consider these examples:

- The PGP Universal Server policy is set to “encrypt if key found, otherwise bounce message”. The handheld user may compose a message to a recipient without a key, but will receive an error when the message is sent.
- Similarly, the handheld user may compose a message using the plaintext “Send Using” option, but the PGP Universal Server policy prevails and the message is sent encrypted. The handheld user is informed as the message is sent.

PGP Universal Server policy will only prevail if the IT policy for “PGP Force Encrypted Messages” is set to “false”. This setting determines whether policy is handheld-based or PGP Universal Server–based and is further described in Table 1 on page 9.

Messages sent from the BlackBerry handheld to multiple recipients are subject to a variety of policy implications. Refer to “Enforcing Policy to Multiple Recipients” on page 12.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

BlackBerry Enterprise Server Setup

Default Policy Attributes

Policy settings should be considered carefully. A post-deployment change to the PGP Universal Server Address will force managed handheld users to re-enroll with PGP Universal Server. Table 1 shows PGP Universal Server policy attributes and their default values.

Attribute	Notes	Default Value
PGP Force Digital Signature	If "False", policy is dictated by PGP Universal Server. If "True", messages composed on the handheld are always signed.	False
PGP Force Encrypted Messages	If "False", policy is dictated by PGP Universal Server. If "True", messages composed on the handheld are forced to encrypt without consulting PGP Universal Server. If no recipient key is found, an error is generated on the handheld.	False
PGP Blind Copy Address	Archival or administrative use. Should PGP-managed messages be blind copied (BCC'd) to a recipient specified by the BlackBerry Enterprise Server administrator? The BCC address is visible on the user's handheld.	False
PGP Allowed Content Ciphers	What ciphers are permitted to encrypt messages? A number in base 2 is displayed based on the selected ciphers.	AES (128-, 192-, 256-bit), CAST, TripleDES
PGP Minimum Strong RSA Key Length	The minimum key length before a user is warned about the length of the RSA key. The default RSA key length used by PGP Universal Server is 2048 bits.	1024
PGP Minimum Strong DH Key Length	The minimum key length before a user is warned about the length of the DH key.	1024
PGP Minimum Strong DSA Key Length	The minimum key length before a user is warned about the length of the DSA key.	1024
PGP Universal Server Address	Used by the handheld to look up policy and the recipient's public key.	None
PGP Universal Server Enrollment Method	0 = enroll by domain username / password 1 = enroll by email sent to user	1
PGP Universal Server Policy Cache Timeout	How many hours can the handheld cache policy after it is retrieved from PGP Universal Server? After cache timeout, the handheld requests policy the next time a message is sent.	24

Table 1: IT Policy Table

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Editing IT Policies

The IT policies for the PGP Support Package for BlackBerry are called the "PGP Application Policy Group". These policies should be modified to conform to corporate security practice. The policies articulated by this guide are recommended by PGP Corporation. Open the BlackBerry Manager on the BlackBerry Enterprise Server. Select the policy group by following the five steps shown below in Figure 3.

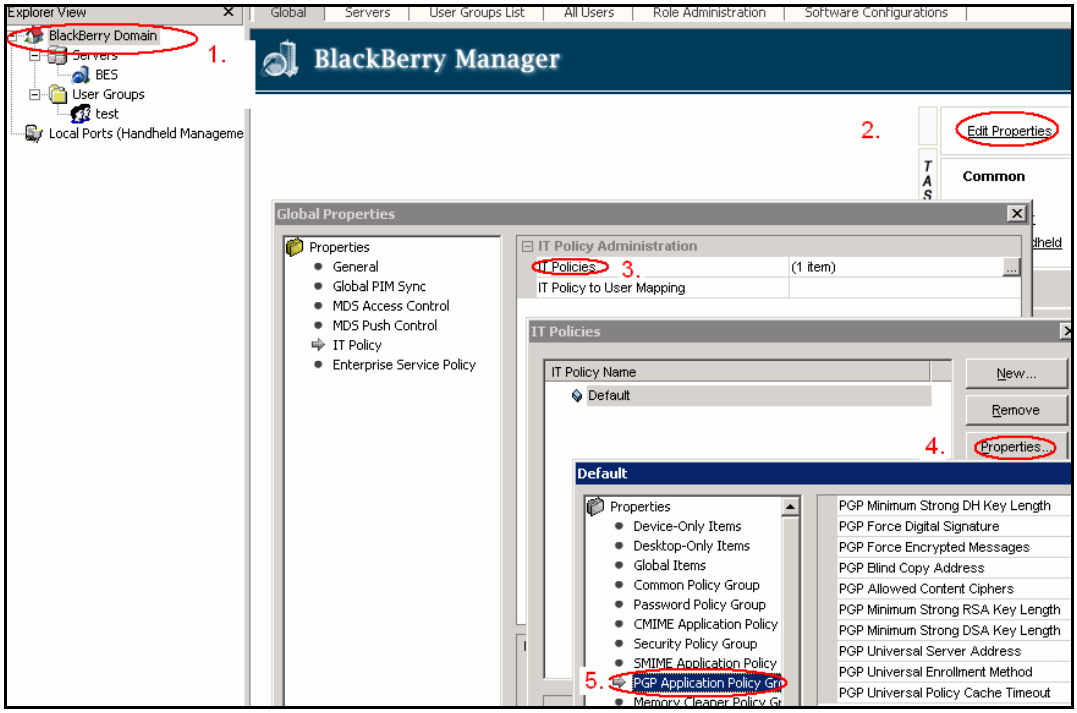


Figure 3: Selecting PGP Application Policy Group

With one exception, PGP Corporation recommends using the default values. The definition of each field is displayed when the field is selected. Table 1 on page 9 explains these fields. For managed users, modify the PGP Universal Server Address to correspond to your managed domain, as shown in Figure 4:

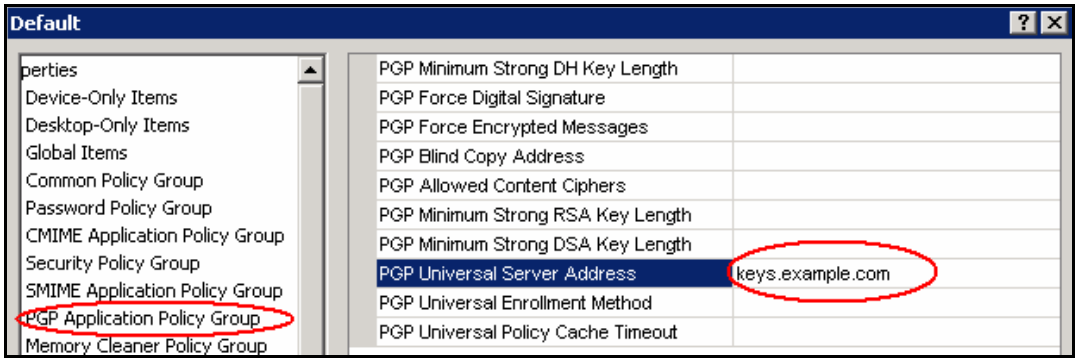


Figure 4: Editing IT Policy

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Enable BlackBerry Enterprise Server Secure Email Support

For BlackBerry Enterprise Server versions prior to 4.1, the PGP Support Package for BlackBerry will not be recognized by the handheld unless S/MIME encryption is enabled on the BlackBerry Enterprise Server. From the BlackBerry Enterprise Server, select “Properties”. Select the “Message Options” tab and enable S/MIME Message Processing, as shown in Figure 5.

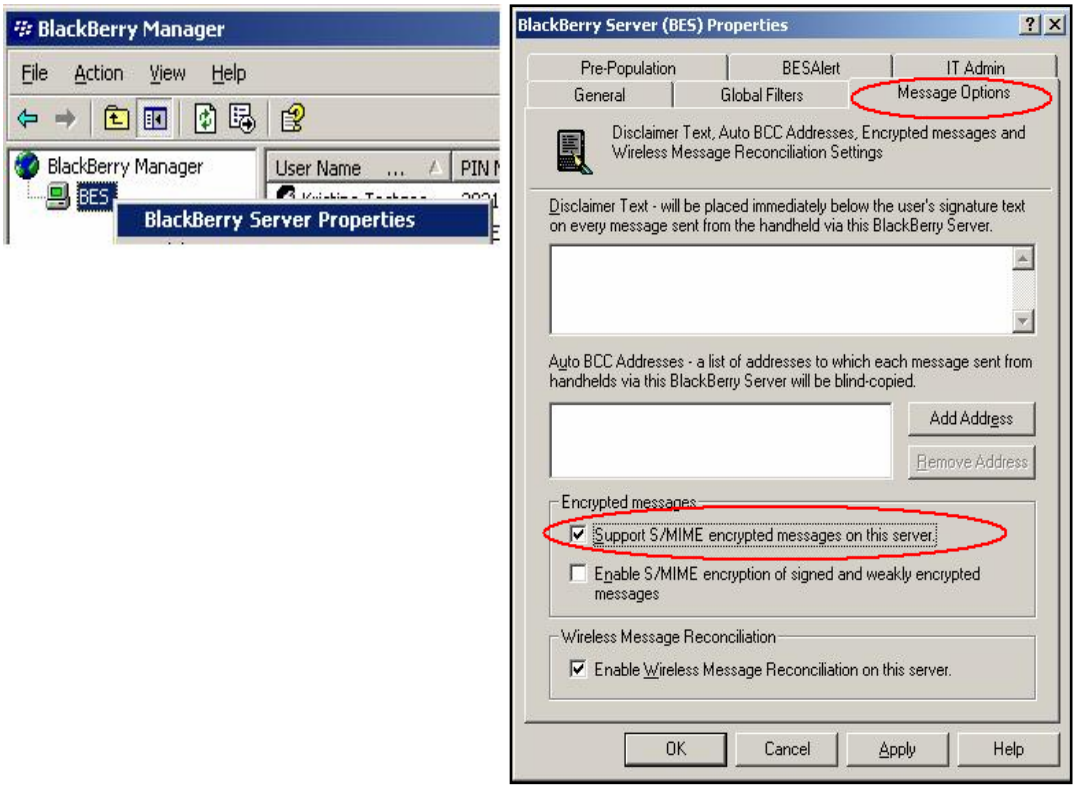

BlackBerry Manager
File Action View Help
BlackBerry Manager
BES
User Name
BlackBerry Server Properties
BlackBerry Server (BES) Properties
Pre-Population
BESAlert
IT Admin
General
Global Filters
Message Options
Disclaimer Text, Auto BCC Addresses, Encrypted messages and Wireless Message Reconciliation Settings
Disclaimer Text - will be placed immediately below the user's signature text on every message sent from the handheld via this BlackBerry Server.
Auto BCC Addresses - a list of addresses to which each message sent from handhelds via this BlackBerry Server will be blind-copied.
Add Address
Remove Address
Encrypted messages
Support S/MIME encrypted messages on this server.
Enable S/MIME encryption of signed and weakly encrypted messages
Wireless Message Reconciliation
Enable Wireless Message Reconciliation on this server.
OK
Cancel
Apply
Help

Figure 5: BlackBerry Enterprise Server 4.0 – Enable S/MIME

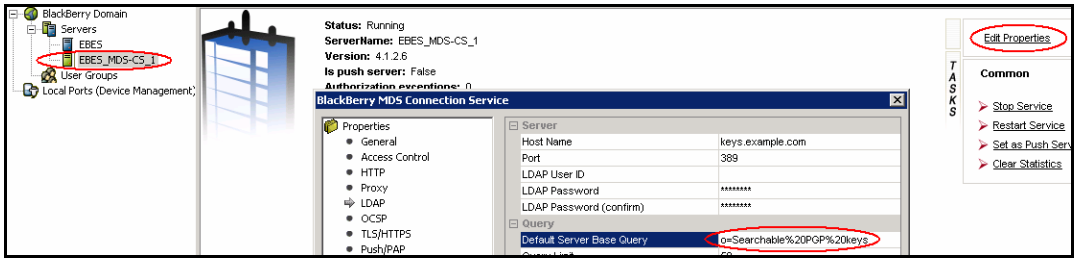


Figure 6: MDS LDAP Settings

All users may also look up keys on an ad-hoc basis using the “PGP Key Search” module that resides on the BlackBerry handheld. This key search is also proxied for the handheld user by the BlackBerry Enterprise Server.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Pushing Policy to the Handheld

- **MDS** – Mobile Data Service (MDS) settings are stored on the BlackBerry Enterprise Server. MDS changes are realized on the handheld whenever MDS-related services are requested.
- **BlackBerry Enterprise Server Properties** – Changes to BlackBerry Enterprise Server properties are sent to the handheld on a regular basis, approximately every 3–5 minutes, depending on server load.
- **IT Policy** – New policies are pushed out after they are created. Modifications to the policy groups are sent every 3–5 minutes, depending on server load. Modifications to IT policy may force handheld users to re-enroll.
- **PGP Universal Server** – PGP Universal Server policy is requested by, not pushed to, the handheld. PGP Universal Server policy changes are requested by the handheld after the policy cache has timed out and a new message is sent. The cache timer is set by IT policy on the BlackBerry Enterprise Server. An unscheduled policy update can be requested by resetting the handheld.

Enforcing Policy to Multiple Recipients

The BlackBerry handheld never transmits more than one copy of a given email message. This behavior preserves bandwidth on wireless networks and simplifies message management on the handheld. A message addressed to multiple recipients will always be transmitted as a single message to the BlackBerry Enterprise Server. If all recipients have keys on the handheld or keys that can be discovered by PGP Universal Server, the message is encrypted on the BlackBerry handheld. However, messages with multiple recipients will likely be addressed to some recipients with keys and some recipients without keys.

For managed users, if the PGP Universal Server “key not found” policy is to bounce messages sent to recipients without keys, the handheld user is prompted to remove the recipient without a key from the distribution list, cancel the message, or supply a key. For all other PGP Universal Server “key not found” policies, a message addressed to recipients with **and** without keys will **not** be PGP-encrypted by the BlackBerry handheld. RIM standard AES encryption will protect the message from the BlackBerry handheld to the BlackBerry Enterprise Server, but PGP Universal Server must be placed in the mail flow to enforce end-to-end policy.

To secure the message internally, “TLS required” should be configured on the BlackBerry Enterprise Server, the mail server, and PGP Universal Server’s outbound mail proxy. For other “key not found” policies such as “Web Messenger” and “Smart Trailer”, PGP Universal Server will transmit multiple copies of the message, as appropriate.

It is possible to put PGP Universal Server directly in the external mail flow so that all messages leaving or entering the enterprise are processed by PGP Universal Server. For large installations, messages are often relayed to PGP Universal Server on a conditional basis. There are many PGP-supported configuration guides available from PGP Corporation to assist with the setup of conditional relay environments.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Handheld Setup

Setup

This section outlines the steps you must perform to activate the PGP Support Package for BlackBerry on your handheld device.

Step 1: Enterprise Activation

A new BlackBerry handheld must first be activated. If the handheld is already able to send and receive messages, proceed to step 2 on page 16. If not, activate the handheld using the process outlined by your administrator. Typically, you will use the “Enterprise Activation” (EA) icon on the handheld.

1. You should have the email address and password assigned to you by your administrator.
2. Using the EA icon, register yourself with the BlackBerry Enterprise Server.
3. Ensure that you can send and receive plaintext email.

Figure 7: Enterprise Activation

© 2006 PGP Corporation. All Rights Reserved.

Step 2: Locate & Install Required Software

Installation of the PGP Support Package for BlackBerry requires four software packages:

Software Package	Provided by	Purpose
BlackBerry Handheld Software	Your administrator or your wireless carrier	Installs prerequisite software onto the handheld.
BlackBerry Desktop Manager	Your administrator, RIM, or your wireless carrier	Used to load the PGP Support Package for BlackBerry.
PGP Desktop Email	Your administrator or PGP Corporation	Send or receive secure email on your desktop PC. Also used to generate your keypair, condition your key, and export it.
PGP Support Package for BlackBerry	Your administrator	Wizard that activates PGP software on your handheld device.
BlackBerry Key Conditioning Preparation Tool (bbkeyprep)	Your administrator	Optional. Automatic key conditioning for keys generated with PGP Desktop Email version 9.5.1 or greater.

If these software packages are not already installed on your PC, please contact your administrator.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Step 3: Install the PGP Support Package for BlackBerry

1. The PGP Support Package for BlackBerry is a wizard that prepares the BlackBerry Desktop Manager for the installation of the PGP software. Run the wizard and accept the licensing terms.
2. Dock the handheld via a mini-USB cable to the PC.
3. Open the BlackBerry Desktop Manager.
4. Launch the Application Loader and make sure the “BlackBerry PGP Support Package” is checked, as shown in Figure 8.
5. Press “Next”. The Application Loader Wizard will enable the PGP Support Package for BlackBerry, and a window will appear to confirm the successful installation.

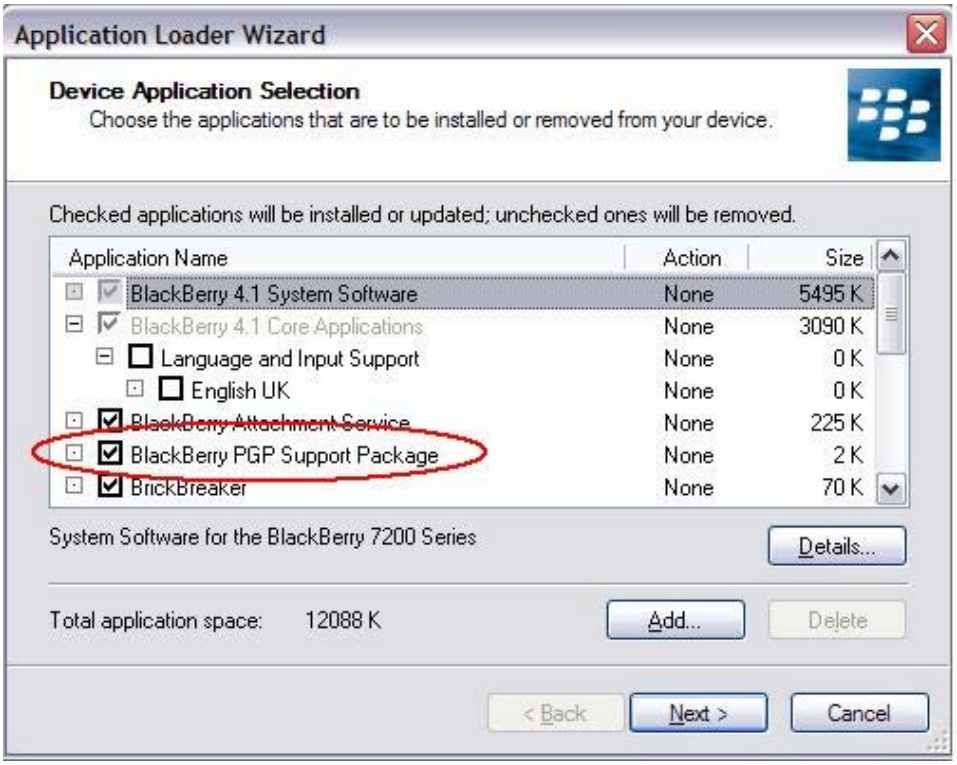


Figure 8: Enable the PGP Support Package for BlackBerry

.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Key Generation & Handheld Import

This process stores your key on your handheld device. The process is unique for managed and unmanaged users. Unmanaged users should follow steps UN-1 through UN-4, beginning on this page. Managed users should follow steps MAN-1 through MAN-4, beginning on page 19.

Unmanaged Users

Step UN-1: Generate the Keypair

1. If you do not already have a keypair, you must create one. Open PGP Desktop Email from the system tray and create a “New PGP Key”.
2. If you already have a keypair you wish to use on your handheld, skip to step UN-2. If not, generate a new keypair. Make a note of the passphrase that will be required when you import the keypair into the handheld.

Step UN-2: Condition the Keypair

If you are responsible for managing your own key and are using a key generated by PGP Desktop Email 9.5.1 or greater, you may use the BlackBerry Key Preparation Tool described in Appendix C on page 46. If your key was generated by PGP Desktop Email 9.5 or earlier, follow the instructions in Appendix B of this guide, starting under the section entitled “PGP Desktop Email: Remove Preferred Keyserver”, on page 38.

Step UN-3: Export & Send Keypair

For unmanaged users, the keypair must be exported and sent to the handheld device.

1. From PGP Desktop Email, right-click on your keypair and select “Export”.
2. You must select “Include Private Key” as shown in Figure 9 so that you can sign messages and decrypt messages sent to your handheld.

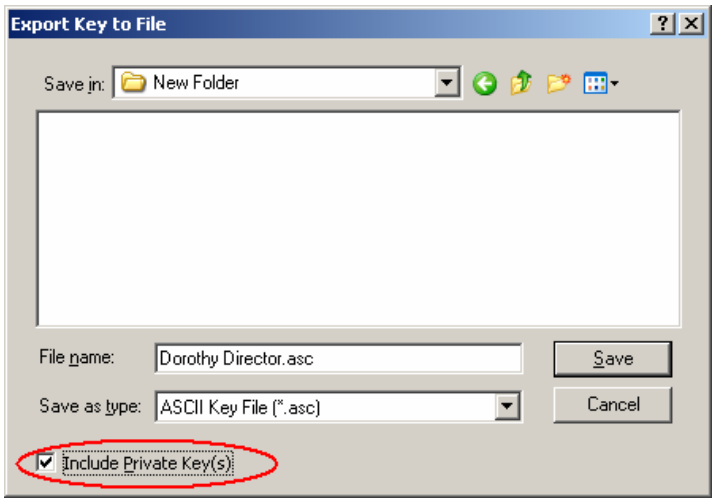


Figure 9: Export Keypair

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

3. Before the keypair is sent to your handheld, you must disable the PGP Desktop Email proxy. This process ensures that a readable, unencrypted copy of your keypair is sent to the handheld. Start by selecting the PGP Desktop icon from the system tray. Uncheck “Use PGP Email Proxy”, as shown in Figure 10. This option will permit the handheld to read the keypair you will send in the next step. You must restart your email program if it is currently open.

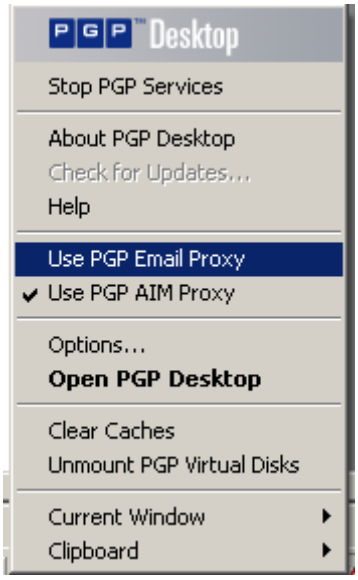


Figure 10: Disable Email Proxy

4. Using the email client on your PC, send the exported keypair to your handheld as an attachment.

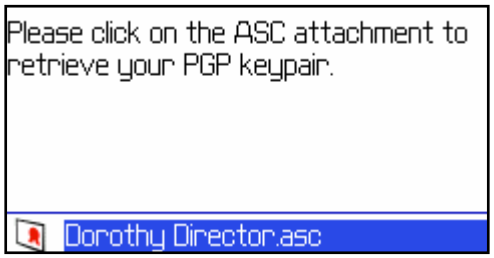
5. Re-enable the PGP Email Proxy.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

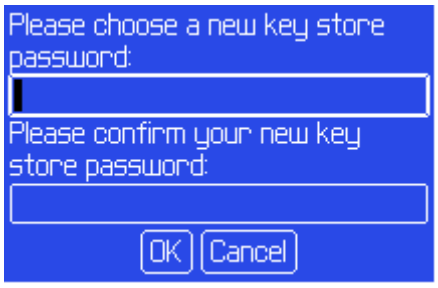
Step UN-4: Import Keypair

1. Using your handheld device, open the email message and click on the attachment. Select “Retrieve PGP attachment”.



2. Once the key has been retrieved, click on the key and select “Import PGP Key”. This key will be saved in your “key store”.

3. Keys stored on the BlackBerry handheld are kept in a “key store.” If you do not already have a key store established on your handheld, you will now be prompted to set the password for your key store. The password must be at least four characters long. If your private key is secured by a passphrase, you will also be prompted for the passphrase associated with your key. The *key store password* is typically **not** the same as the *passphrase* you would have assigned to your private key at the time you generated the keypair.



4. If your keypair is secured with a passphrase, you will be prompted to enter it now.
5. Your key has now been imported successfully. There is no dialog box confirming that your key has been imported. If you wish to manually confirm that your keypair has been imported, select “Options” from the handheld’s main menu. Select “Security Options”, and then “PGP”. Your key should be displayed as the “Default Key”.
6. Re-enable the PGP Email Proxy. Refer to Figure 10 on page 17.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Managed Users

Step MAN-1: Enroll with PGP Universal Server

Before beginning this process, all keys for all users must be conditioned as described on page 6. Detach the BlackBerry handheld from the PC. Before the BlackBerry handheld is enrolled with PGP Universal Server, your system administrator must ensure that your keypair has been loaded onto the server. Enrollment may then be performed Over the Air (OTA). Ensure that your radio is on. You may receive a prompt requesting that you enroll with PGP Universal Server. If not, you will be prompted to enroll when you attempt to send a message. Alternatively, select “Options”, “Security Options”, and “PGP”, as shown in Figure 11:

Figure 11: Enroll with PGP Universal Server – Step 1

Because the handheld is not yet enrolled, there is no default key displayed, as shown on the left-hand panel in Figure 12. Click the track wheel and select “Enroll with Universal Server”. Your email address should already be filled in. If your email address is not correctly displayed, your BlackBerry handheld has not successfully completed Enterprise Activation. Please contact your administrator.

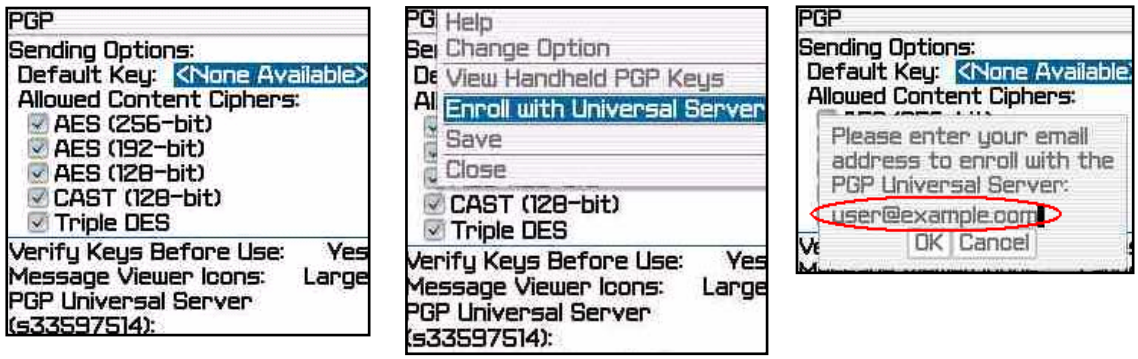


Figure 12: Enroll with PGP Universal Server – Step 2

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

There will be a brief delay before the process begins. After the enrollment is successful, you will be asked to download your private and public keys, as shown in Figure 13.

PGP
You have successfully enrolled with the PGP Universal Server. Would you like to download your keys from the server now?
Yes
No
PGP Universal Server (Desktop):

Figure 13: Enroll with PGP Universal Server – Step 3

Step MAN-2: Store Keys in Key Store

Private keys stored on the BlackBerry handheld are kept in a “key store.” To maintain the security of your private key, you must establish a password for your key store, as shown in the left-hand panel of Figure 14. The password must be at least four characters long. Once you have created the key store, you must grant permission for the enrollment application to access the key store, as shown in the right-hand panel below.

Send Using: PGP Universal Default
Please choose a new key store password:
Please confirm your new key store password:
OK
Cancel
Send Using: PGP Universal Default
The following application is requesting access to your PGP Key Store. Your personal keys have been downloaded and will be added to your key store.
OK
Cancel
Vendor Name:
Research In Motion Ltd.

Figure 14: Save Keypair in Key Store

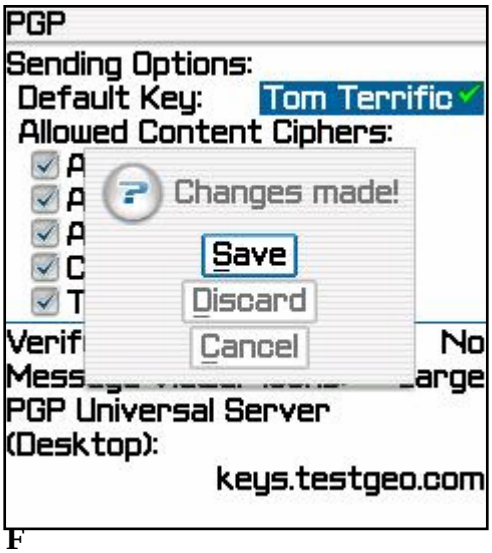
© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

If your private key is secured by a passphrase, you will be prompted for the password associated with your key, as shown in Figure 15. This second password may be different than the key store password you just created.

Figure 15: Save Key Store – Step 1

After the key store has been populated, an "enrollment complete" message will appear. Press "OK". Because the PGP options have been changed, you must save them when you exit this menu, as shown in Figure 16.



F

Figure 16: Save Key Store – Step 2

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Managing Public Keys

Your public and private keys are now stored on the handheld. However, a secure message can only be sent after the handheld acquires the public key of the recipient. For PGP Universal Server–managed users, this process is generally managed by PGP Universal Server. For unmanaged users, your handheld must acquire these keys and you must save them in the key store and mark them as trusted before they can be used. Public keys can be obtained from several places:

- On a keyserver specified by the handheld. This lookup can also occur as you send mail.
- Using an email program or PGP Desktop Email, a public key can be sent to any handheld. This process is described below.
- A public key can be sent from one handheld to another. This procedure is described in “Importing a Public Key from a Handheld” on page 23.

Importing a Public Key via Email

The steps required to acquire an existing public key from a correspondent are similar to those described in Step UN-3 on page 16.

1. Correspondents should disable the PGP Email Proxy on the PC.
2. As shown in Figure 17, they can use PGP Desktop Email to easily mail their public key. Alternatively, they can create an email message with their public key attached.

Figure 17: Send Public Key via PGP Desktop

3. After you have received the email on the handheld, select the attachment and save the key into the key store.
4. Mark the public key as trusted. This procedure is further described in “Trusting a Public Key” on page 23.
5. Re-enable the PGP Email Proxy.

Importing a Public Key via a Keyserver

If many of your correspondents have published their keys on a publicly accessible keyserver, you should establish their keyserver as your default. Start by following the “Specifying Keyservers” procedure on page 28. After their keyserver is set up as the default, any attempt to send an encrypted message to a recipient without a key will be proceeded by a lookup of the default keyserver.

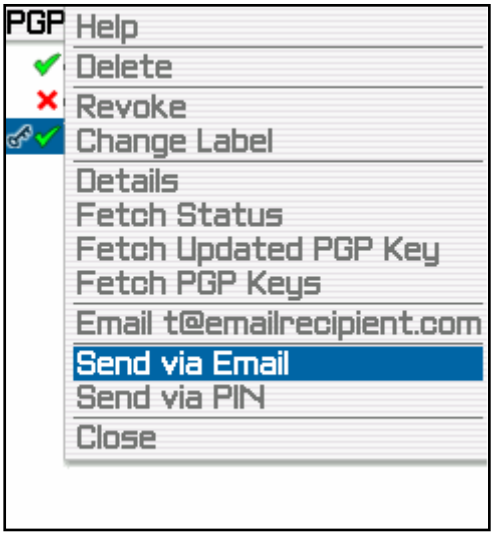
If the key is found, it must be imported onto the handheld and marked as trusted before it can be used to encrypt a message.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Importing a Public Key from a Handheld

A public key that you have on your handheld can be easily mailed to another handheld. The recipient can then import the key into his or her key store.



1. On the handheld, select “Options/Security Options/PGP Keys”.
2. You will see a list of keys in the table. Select the key you wish to send.
3. Select the “Send via Email” option to send the key, as shown at right.
4. Select an address from the address book.
5. Send the email in plaintext.
6. On the receiving handheld, import the key into the key store.
7. Mark the public key as trusted as described in the following section, “Trusting a Public Key”.

Trusting a Public Key

For unmanaged users, once a key has been loaded into the key store, it must be marked as trusted before it can be used. The trust status is indicated by the icon to the left of the key. To display your key store, select “Options/Security Options/PGP Keys”.

A red “x” indicates the key is **not** trusted. A green check mark indicates the key **is** trusted. Select the untrusted key and then select “Trust”.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Sending & Receiving Email

Sending Email

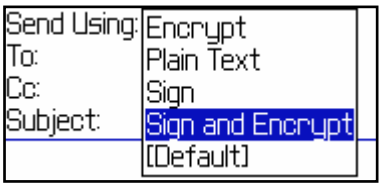
Once you have installed the PGP software and the needed keys onto the handheld, you may begin sending mail.

If you are a managed user, your administrator determines how outgoing messages are processed. Unmanaged users have the option of sending email that is unencrypted, encrypted, and/or signed. For unmanaged users, the default “Send Using” option is “Plain Text” for recipients without keys and “Encrypt” for recipients with keys. This option can be modified to determine how the message is coded. You can always override this option before you send a message.

Copies of all sent messages are saved on the handheld. For privacy, mail sent as encrypted is also stored as encrypted on your handheld device. Sent messages are encrypted with your public key.

Setting “Send Using” Default Option

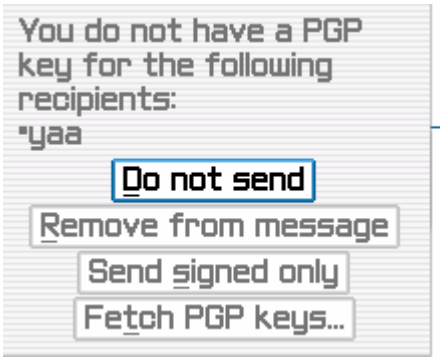
Unmanaged users can change the default security option as you compose your message, select “Send Using”. Click the track wheel and select “Change Option”. In the example shown at right, the message format has been changed from “Encrypt” to “Sign and Encrypt”.



Sending a Message

For unmanaged users, all required keys must be present in the key store before a secure message is sent. You will need a public key for each recipient and your own private key if the message is signed. The needed keys for managed users are generally gathered by PGP Universal Server. There are multiple scenarios when sending an encrypted message:

- All required keys are already in the key store or available to PGP Universal Server—the message is processed and sent.
- You are attempting to send an encrypted message and the public key for the recipient is not available. If a default keyserver has been defined (see “Specifying Keyservers” on page 28), you can easily locate the recipient key using “Fetch PGP keys”. Assuming you can locate the key, you can send the message after you save the key in your key store and trust it.
- For unmanaged users, a secure message is being sent to one or more recipients, and the key for at least one recipient is not in the key store, or is not trusted, and is not on the default keyserver. It is also possible that one of the recipients does not possess a public key. In any case, the message will not be sent to any recipients until all public keys have been added to the key store. You may remove keyless



© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

recipients from the distribution list, sign (but not encrypt) the message, or choose to send the message in plaintext.

- For managed users sending to one or more recipients without a key, your administrator determines if the entire message distribution is sent or blocked.

Replying to a Message

Replying to a message is similar to sending a new message, with the following exceptions:

- By default, the message will be sent using the same “Send Using” options used in the incoming message.
- The recipient address has already been determined and is placed into the “To” field.
- If the message has an attachment, it will not be part of the reply.

Receiving Email

Incoming messages may be:

- Plaintext
- Signed, encrypted, or both
- Received with one or more attachments. The handheld is not able to receive encrypted attachments, which are displayed as:

To decrypt an encrypted message, your private key must be in the handheld key store. To authenticate a signed message, the public key of the sender must be available.

Various scenarios are possible for encrypted messages:

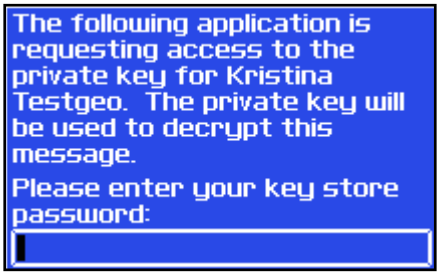
- **All required keys are present:** the message is decrypted and authenticated (if it has been signed by the sender).
- **A required key is missing:** the message is not read and the error message indicates the missing key.
- **There is an encrypted attachment:** such an attachment cannot be read by the handheld.
- **The attributes of your public key were not set properly:** the message cannot be decrypted.

When a message is received, the leftmost column of the mailbox on the BlackBerry handheld displays a variety of icons, as shown at left. A lock symbol will appear to the left of encrypted and/or signed messages. Your private key is required to open an encrypted message.

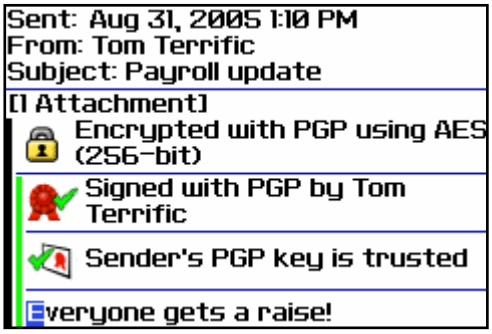
© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

When opening messages, you will occasionally be prompted for your key store password, as shown at right. The default timeout for this request can be changed as described in “Modifying the Key Store Password Timeout” on page 27.


The following application is requesting access to the private key for Kristina Testgeo. The private key will be used to decrypt this message.
Please enter your key store password:

Once the message is decrypted, a series of icons is displayed just beneath the subject line. These icons verify the confidentiality of the transmission and the authenticity of the sender. In the example at right, the message was decrypted successfully and the signature has been verified by the BlackBerry handheld. (This example uses “large icons”.)


Sent: Aug 31, 2005 1:10 PM
From: Tom Terrific
Subject: Payroll update
[1 Attachment]
Encrypted with PGP using AES (256-bit)
Signed with PGP by Tom Terrific
Sender's PGP key is trusted
Everyone gets a raise!

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Key Management

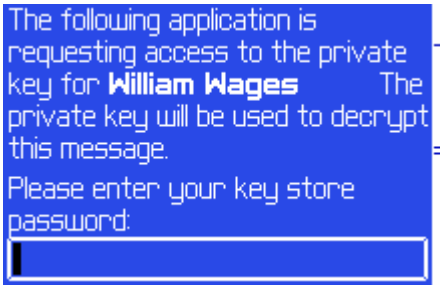
For unmanaged users, all keys that you wish to use must be saved on your handheld. Public keys are used to send an encrypted message or validate the signature of a received message. Private keys are used to decrypt a received message, read your sent mail, or sign a message. You must acquire the key via email or locate the key on a keyserver. The key must then be stored on the local key store and marked as trusted.

The features discussed in this section pertain to advanced users who may wish to:

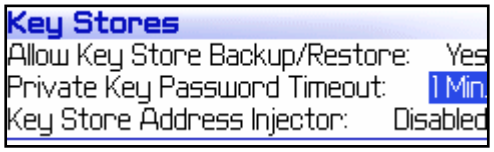
- Modify the default key store password cache timeout
- Specify alternate keyservers for future searches
- Locate and store keys on an ad-hoc basis
- Update keys on the handheld
- Publish their PGP Desktop Email key to the PGP® Global Directory

Modifying the Key Store Password Timeout

By default, the password associated with your key store is cached on the handheld for 1 minute. After 1 minute of inactivity, any request for keys within your key store will generate the message shown at right.


The following application is requesting access to the private key for **William Wages** The private key will be used to decrypt this message.
Please enter your key store password:

The default key store timeout can be modified by selecting “Options” from the main menu, then “Security”, and then “Key Stores”. Select the “Private Key Password Timeout” and change the value as desired. Your administrator can also modify the default password timeout.

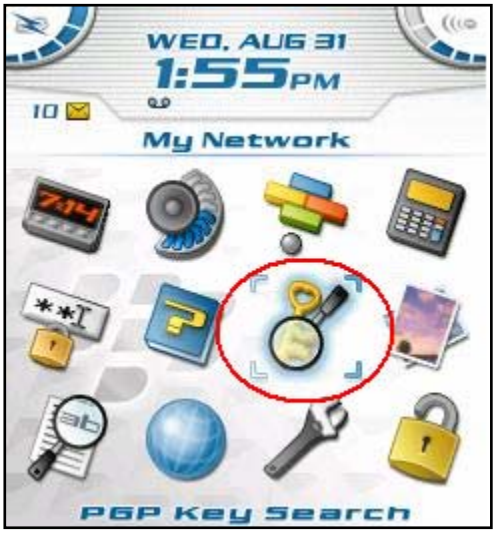


© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Specifying Keyservers

A secure message can only be sent after the BlackBerry handheld acquires the public key of the recipient. If you do not already have the key of the recipient stored on your handheld, the key can be located using the “PGP Key Search” function on the main menu of your BlackBerry handheld, as shown at right.

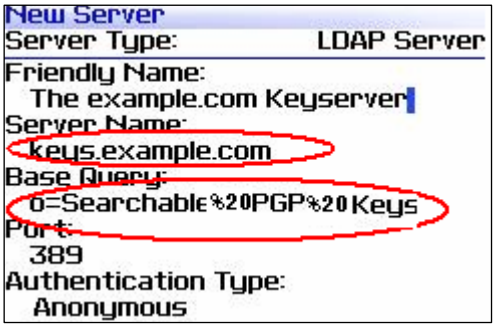


To download a key from a keyserver, you must first define a new keyserver. Select the <Default> server and click the track wheel. Select “New Server”, as shown at right.

Note that the Base Query

o=Searchable%20PGP%20Keys

is case-sensitive and must be entered precisely as shown at right, starting with a lower-case “o”. To search *legacy* PGP Universal Servers version 1.22 or lower, the Base Query should be “o= PGP Keys”. The “Friendly Name” lets you distinguish multiple keyservers from one another.



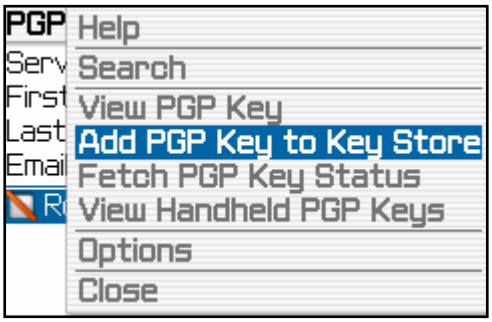
After the keyserver is defined, it becomes the default for all ad-hoc key searches. Your administrator can also specify the default LDAP server.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Locating & Saving Ad-Hoc Keys

With the alternate keyserver defined and selected, enter all or a portion of the name or email address of the recipient whose key you wish to locate. The key search is performed and the key must be saved on the BlackBerry handheld. Once the key has been located, it should be saved. Once a key has been loaded into the key store, it must be marked as trusted before it can be used. See “Trusting a Public Key” on page 23.



Updating Keys in the Key Store

You might need to update a key in the key store either because the key has changed or has expired. To update any key, you must first delete the existing key from the key store. Once you have deleted the existing key, you may then follow the appropriate procedure to re-import the key.

PGP Global Directory

How will your correspondents locate your public key so that they may send you encrypted messages? The PGP Global Directory is a free, publicly available keyserver hosted by PGP Corporation. The PGP Global Directory permits PGP users to find the public keys of more than 50,000 PGP users with whom they may wish to exchange secure messages.

If you would like to publish your public key on the PGP Global Directory, please visit https://keyserver.pgp.com/

An alternate method of publishing your key is to use PGP Desktop Email’s “send key” feature. However, this feature, shown in Figure 18, should be avoided because it changes the “preferred keyserver” attribute of the published key. This change will signal recipients that you are able to receive PGP MIME–based attachments, which cannot currently be read on the BlackBerry handheld.

Figure 18: Post Public Key Using PGP Desktop Email

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Appendix A: Troubleshooting

Server-Based Troubleshooting

BlackBerry Enterprise Server Log Files

The BlackBerry Enterprise Server logs provide a wealth of information. You can find the logs in this directory:

\Program Files\Research In Motion\BlackBerry Enterprise Server\Logs

A separate directory is created for each day of activity. Ten log files are created by default.

PGP Universal Server Logs

PGP Universal Server logs are broken into nine distinct sections. The most useful log for troubleshooting BlackBerry Enterprise Server configurations is the “Client” log.

Troubleshooting Enrollment

Figure A-1 catalogs the successful PGP enrollment of a user. The five log entries read from the bottom up and are translated as follows:

1. The Mobile Data Service (MDS) (10.214.0.66) logs in on behalf of the user.
2. The PGP enrollment request is received.
3. The user is recognized as a managed PGP Desktop Email 9.5 user.
4. The keypair is sent to the MDS so it can be delivered to the handheld.
5. The connection is closed.

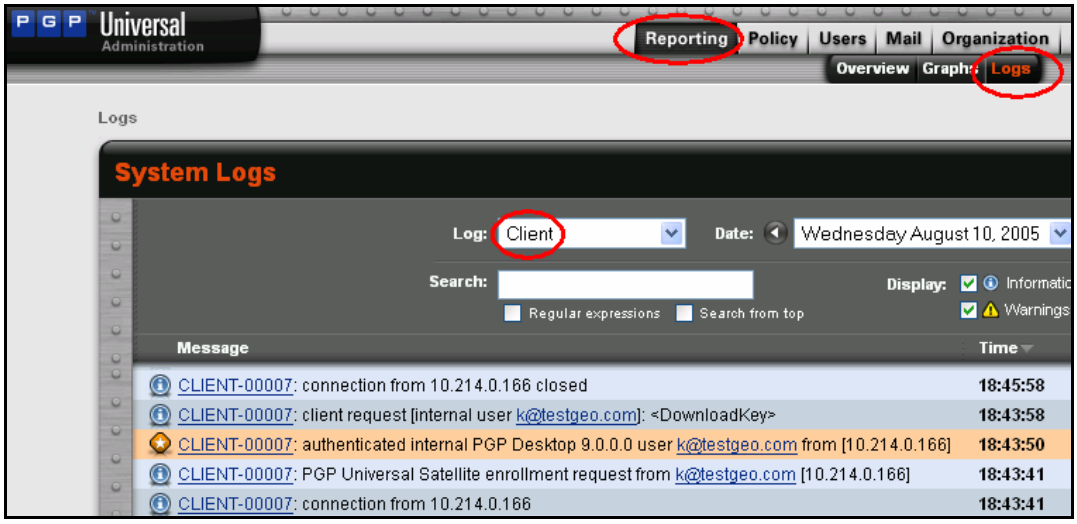


Figure A-1: Successful User Enrollment

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Tracing Key & Policy Lookup

Figure A-2 traces a successful policy and key lookup. Reading from the bottom up:

1. The MDS connects to PGP Universal Server.
2. The connection is on behalf of the handheld. The handheld user in this example is sending a message to pgp.com, which is external and not managed by this server. What policy should be applied when the handheld user is sending to an external unmanaged domain?
3. Three seconds later: The reply sent by PGP Universal Server was “encrypt if you can find a key”. However, the public key is not stored on the BlackBerry handheld. The BlackBerry handheld requires a key, and the MDS proxies this key request to PGP Universal Server.
4. Five seconds later: This PGP Universal Server queried **keys.pgp.com**. **keys.pgp.com** returned the public key of the recipient. This key is sent to the MDS, which sends it to the handheld, which then encrypts and sends the message.

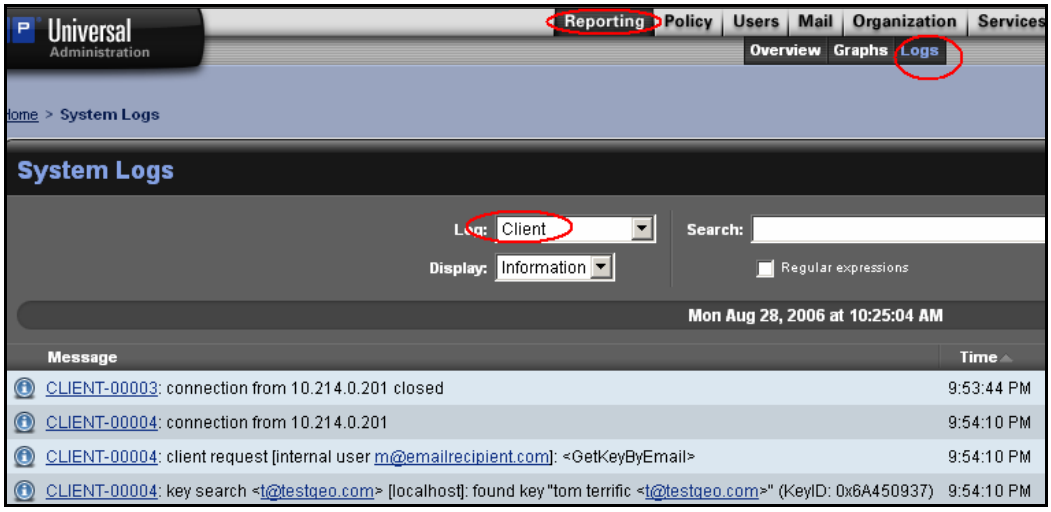


Figure A-2: Successful Policy & Key Lookup

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Managed User Cannot Enroll with PGP Universal Server

- **MDS availability –** Can the handheld browse to a common Internet site? If not, the MDS may not be set up properly.
- **PGP Universal Server availability –** If deployed, verify that the BlackBerry Enterprise Server can make an outbound connection to the PGP Universal Server on port 443.
- **PGP Universal Server user –** Check to see if the email address matches the name of the user listed in PGP Universal Server's list of "Internal Users" and that **two** key icons are present. The padlock icon shown in Figure A-3 indicates that Tom Terrific is a GKM user.

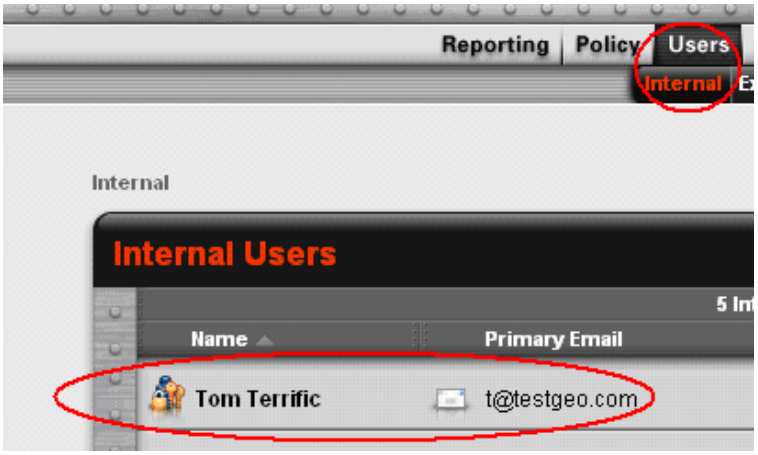


Figure A-3: Validate Name & Keypair

If the handheld is unable to enroll successfully, ensure that:

- The handheld has successfully completed Enterprise Activation
- The BlackBerry Enterprise Server displays the user's PIN and "running" status, as shown in Figure A-4

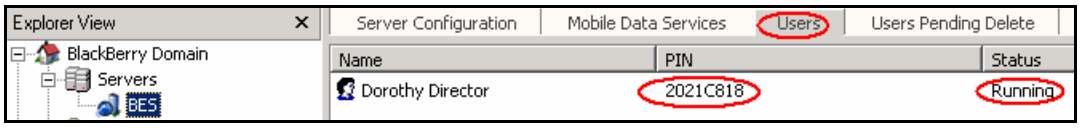


Figure A-4: Active BlackBerry Enterprise Server User

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Handheld-Based Troubleshooting

Incorrect Passphrase

If a user's key is secured with a passphrase, and the user is unable to install his or her key, he/she may receive the error message shown at right. There are two possibilities:

1. The user has incorrectly entered his or her passphrase.
2. The key was created using PGP Desktop Email 9.5.

For the second problem, PGP Desktop Email 9.5 keys must be rewritten. There are two possible solutions. The first is to remove the passphrase from the private key using any version of PGP Desktop. If a passphrase-secured key is required, the key must be rewritten using PGP Desktop 9.0 or earlier, exported, and re-installed in the handheld device.

"Your PGP Universal Server policy is out of date and could not be updated"

This message indicates that the handheld user's key has expired. Condition the key so that the expiration date is set to "Never", as shown in "Manual Key Conditioning" (Appendix B) on page 36.

Email on Handheld is Blank or Cannot be Decrypted

The attributes associated with a user's public key are used by the sender to determine the appropriate options to secure a message. This negotiation process ensures a sender does not encrypt a message in a way that is unreadable by the recipient.

If a user is unable to read a message on the BlackBerry handheld, but can read the message using PGP Desktop Email or PGP Universal Satellite, it is likely the recipient's key is not properly conditioned. Ensure that the key:

- Does **not** have a "Preferred Keyserver" set
- Only supports the AES256, AES192, AES128, CAST, & TripleDES ciphers
- Does **not** support Bzip2 compression

For details on how to change and publish these attributes, see "Manual Key Conditioning" (Appendix B), beginning on page 36.

If these steps have already been taken, it is possible the sender is using an old copy of the recipient's key. Determine the source of the key and send a new copy of the conditioned public key to the sender.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

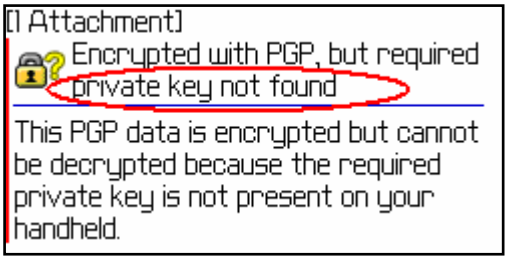
Problems Sending Encrypted Email

- For unmanaged users, is the public key of the recipient stored on your handheld? If it cannot be found at send time, you must acquire the public key, add it to the key store, mark it as trusted, and then send the message.

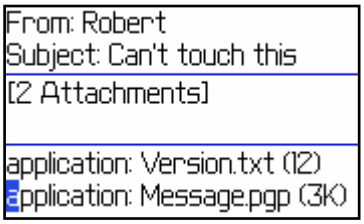
- For unmanaged users, if the sender's key is in your key store but you receive the message shown at right, the public key of the recipient is not trusted. You must mark it as trusted (as described in "Trusting a Public Key" on page 23) before you send the message.

Incoming Email is Encrypted

- Have you downloaded a copy of your public **and** private keys onto your handheld? If not, the incoming message may be encrypted and unreadable, as shown at right. For unmanaged users, if you exported your key to your handheld, you may have failed to click the checkbox shown in Figure 9 on page 16.


[1 Attachment]
Encrypted with PGP, but required private key not found
This PGP data is encrypted but cannot be decrypted because the required private key is not present on your handheld.

- If the incoming email appears as an attachment that cannot be read, your public key may possess attributes that are not supported by the BlackBerry handheld. Check your public key attributes (see Appendix B: "Manual Key Conditioning", beginning on page 36). Then republish your key.



- If the message cannot be decrypted, the sender and receiver may be using different versions of your key. The sender should import the current version of your key to the key store and clear any cache that may be presenting an old version of your public key.
- If an attachment cannot be read, it may be encrypted. The handheld is not capable of decrypting attachments. Inform the sender to send attachments in plaintext or read the message via your desktop email client.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Cannot Authenticate Sender

- If the message cannot be authenticated, the public key for the sender may not be present in the key store. Check your key store, locate the sender's public key, send it as an unencrypted attachment to your handheld, import it, trust it, and re-read the signed message.

Expired Key

- Ensure that the date and time are set correctly on the handheld by selecting "Options" from the main menu, and then "Date/Time".

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Appendix B: Manual Key Conditioning

For managed users, if the user's private key is held without an individual passphrase on the PGP Universal Server, the user is said to be in Server Key Mode (SKM). All SKM keys can be conditioned centrally using PGP Universal Server's administrative interface and PGP Desktop Email. If the desktop user and PGP Universal Server hold a user passphrase–protected copy of the key (called Guarded Key Mode [GKM]), the administrator will have to visit every GKM client and condition each user's GKM key. For unmanaged users, a privately held key (called Client Key Mode [CKM]) is stored within a user's keyring. This keyring is accessed only via PGP Desktop Email. Appendix C describes a tool that can be used to condition CKM and GKM keys. If this is inapplicable, see page 16. Why is key conditioning required? There are several reasons.

PGP MIME is the default sending format for PGP Desktop Email and other PGP applications. PGP MIME ensures message fidelity and is further described here: http://www.ietf.org/rfc/rfc2015.txt However, PGP MIME–encoded messages cannot be read on older software versions of the BlackBerry handheld. In this case, the "preferred server" attribute should be cleared from each user's keypair before the keypair is downloaded to the handheld. When a sender locates a key without this attribute, the sender will not encode the message using PGP MIME.

Bzip2 is an open source data compression algorithm. Bzip2 is not supported on the BlackBerry handheld, so Bzip2-compressed messages cannot be viewed on the handheld. To lessen the likelihood of receiving a Bzip2-compressed message, each user's key should exclude Bzip2 compression. Only keys created on PGP Desktop Email for the Macintosh will have Bzip2 enabled by default.

The supported ciphers on the BlackBerry handheld are AES256, AES192, AES128, CAST, and TripleDES. Mail encrypted by other ciphers (such as IDEA or Twofish) cannot be deciphered on the handheld. Support for IDEA and Twofish should be removed from all keys of all BlackBerry handheld users.

After these operations are completed, users may still receive unreadable encrypted messages or attachments if external users encrypt to a copy of the old, unconditioned key. In this case, the user will have to read the message at the desktop. The recipient or administrator should make the modified key available to the sender.

Unmanaged users should now skip to "PGP Desktop Email: Remove Preferred Keyserver" on page 38.

SKM Key Conditioning

During an email outage window, the administrator exports private and public keys from PGP Universal Server to a PGP Desktop Email host. After the keys are exported, PGP Desktop Email is used to change the attributes of the keys. The original key is removed from PGP Universal Server, the public key and email key cache are cleared, and the conditioned key is re-imported into PGP Universal Server.

An outage window is required during the brief period between the deletion of the original key and the importation of the newly conditioned key. When no key is present, outgoing mail detected by PGP Universal Server triggers the generation of a new keypair. The outage prevents the generation of this second keypair.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

PGP Universal Server: SKM Export

This procedure should also be followed for all new users. Use one computer to access both PGP Universal Server and PGP Desktop Email, if possible. From PGP Universal Server, export some or all users, as shown in Figure B-1.

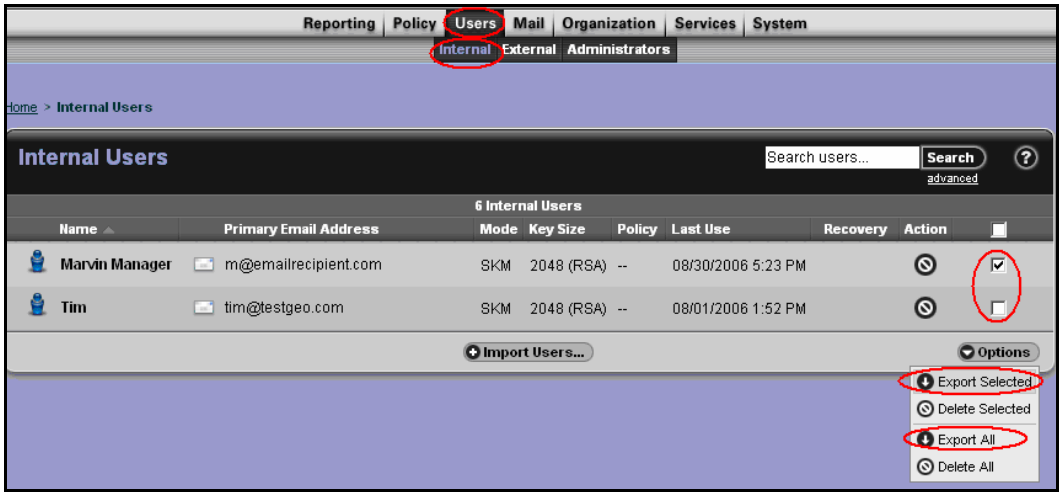


Figure B-1: Export SKM Users

To export the entire keypair, select “Export Private Key”, as shown in Figure B-2:

Figure B-2: Export SKM Keypair

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

PGP Desktop Email: SKM Import

After all keys have been exported, move the PGP Armored file to the desktop of the PGP Desktop Email machine. Double-click on the file and import all keys, as shown in Figure B-3:

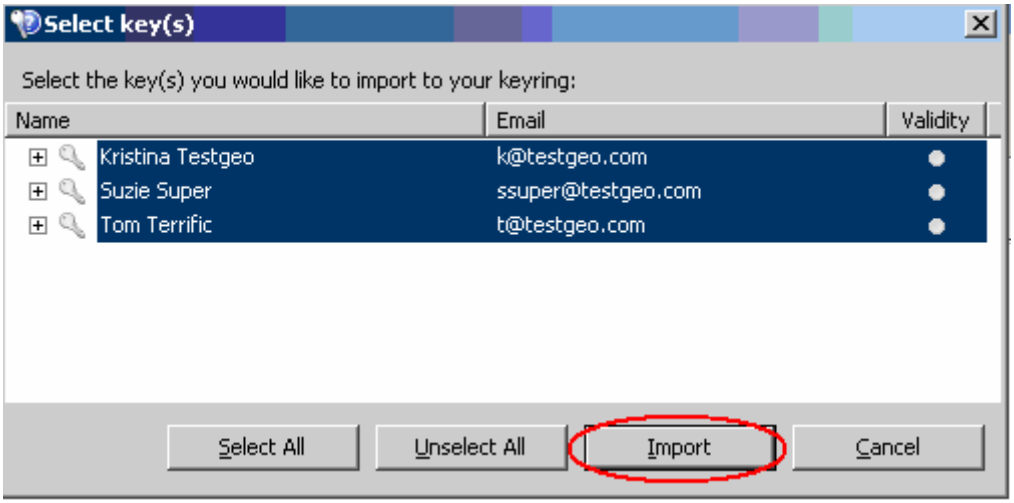


Figure B-3: Import SKM Keys

PGP Desktop Email: Remove Preferred Keyserver

Removing the “Preferred Keyserver” ensures that the handheld will not receive PGP MIME messages. Open PGP Desktop Email and select “PGP Keys”. If you are conditioning keys for multiple users, press Ctrl-A to select “All Keys”, as shown in Figure B-4. If you are conditioning only your keypair, select your own key. In either case, right-click and select “Key Properties” (not shown).

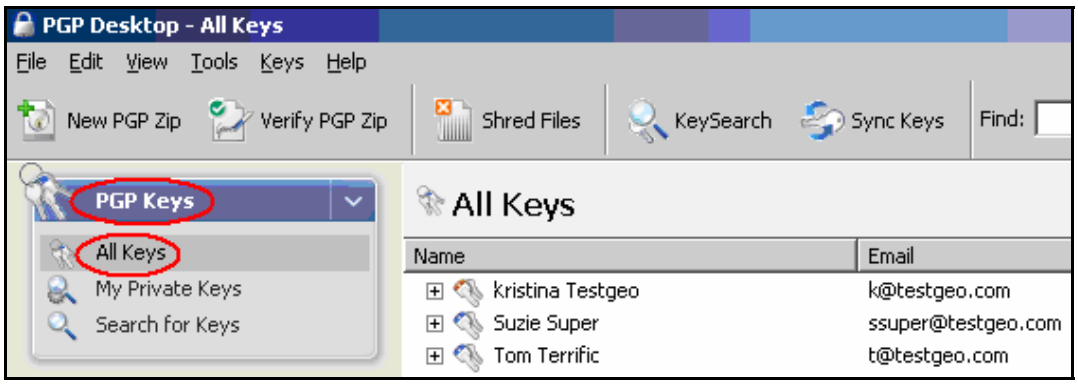


Figure B-4: Remove Preferred Keyserver – Step 1

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

An individual pop-up screen displays the properties for each user, as shown in Figure B-5. Click on the “Keyserver” attribute.

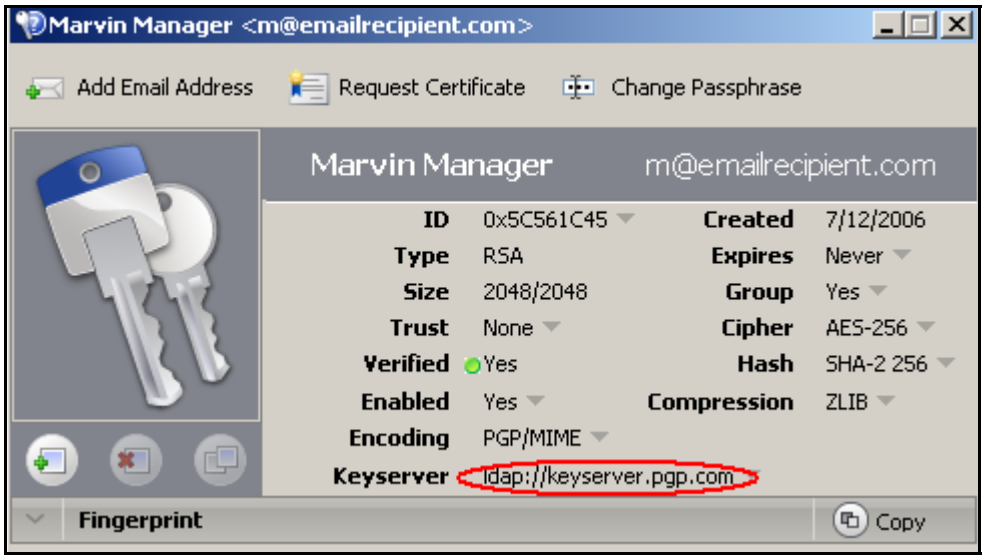


Figure B-5: Remove Preferred Keyserver – Step 2

Delete the contents of the “Server” field and press “OK”, as shown in Figure B-6:

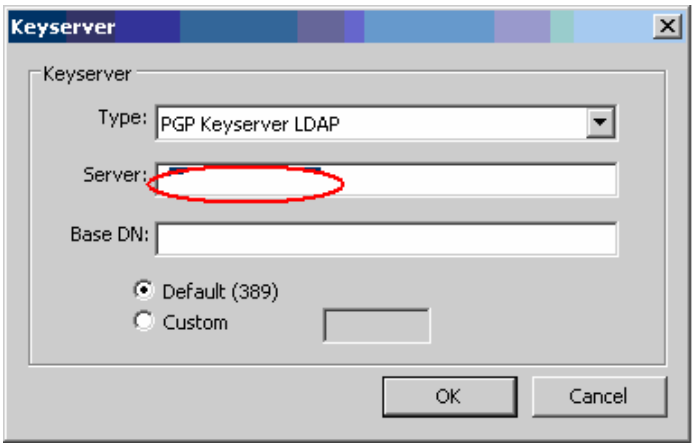


Figure B-6: Remove Preferred Keyserver – Step 3

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Remove Bzip2 Compression

Bzip2 is not supported on the BlackBerry handheld. By default, keys that are generated by PGP Universal Server or PGP Desktop Email for the PC do not have Bzip2 compression enabled. To ensure Bzip2 is not enabled on each user's key, select the "Compression" attribute shown in Figure B-7 and make sure Bzip2 is unchecked.

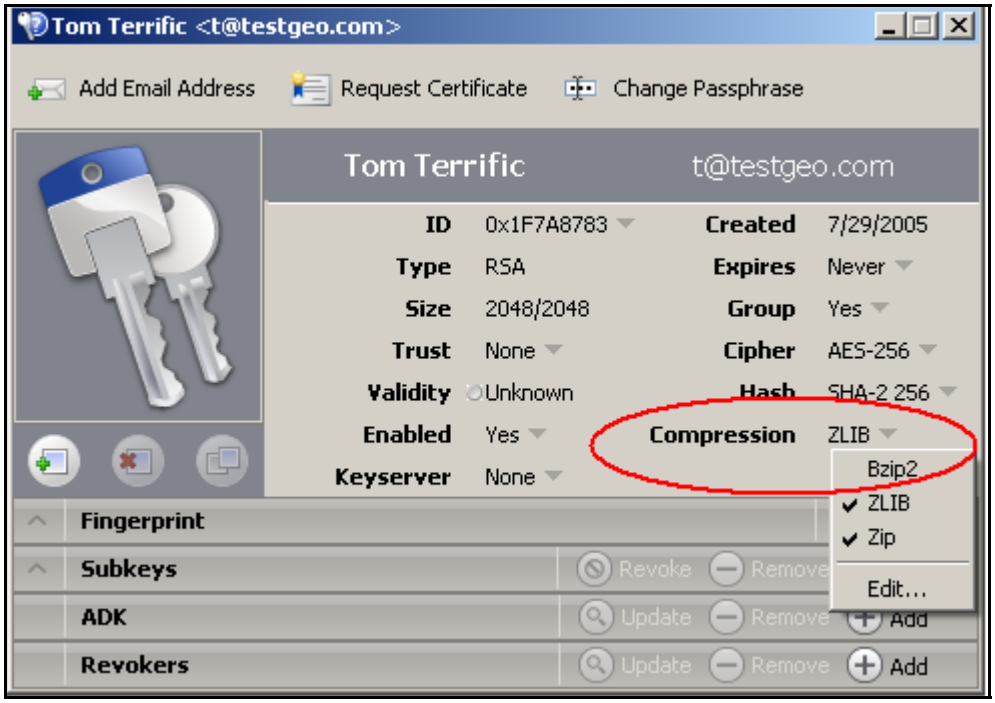


Figure B-7: Remove Bzip2 Compression

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Remove Unsupported Ciphers & Remove Key Expiration

IDEA and Twofish should be grayed out so that you do not advertise the ability to accept ciphers that the handheld software cannot decrypt. Select the “Edit” button, as shown in Figure B-8, and uncheck IDEA and Twofish. If the “Preferred Keyserver” attribute was removed, this key will not automatically renew. Ensure that the expiration date of the key is set to “Never”.

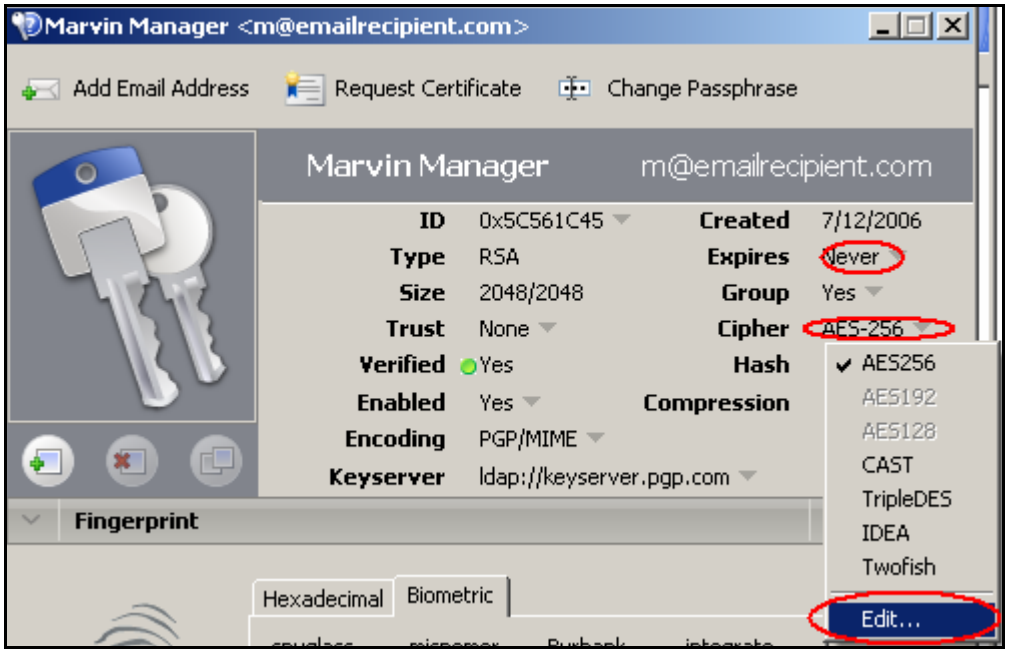


Figure B-8: Remove Unsupported Ciphers, No Expiration Date

For unmanaged users, the conditioning process is now complete.

PGP Desktop Email: Export Keys

Once you have conditioned each key, select the keys you have conditioned and export the private and pubic keyring, as shown in Figure B-9:

Figure B-9: Export Keyrings

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

PGP Desktop Email will automatically create one file for the public keys and one for the private keys. The default names are pubring and secring, respectively. The file can be placed on the desktop by selecting the ellipse, as shown in Figure B-10:

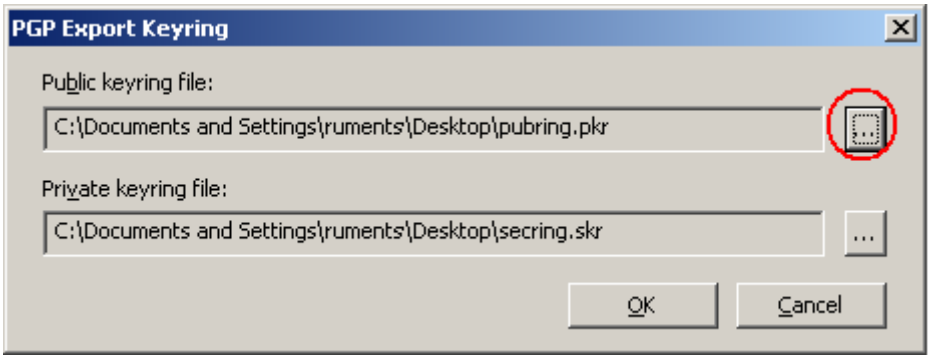


Figure B-10: Save Exported Keyrings

PGP Universal Server: Delete & Import Keys

Initiate an email outage so that no messages are sent to PGP Universal Server. Login to PGP Universal Server. As shown in Figure B-11, delete some (or all) internal users whose keys are to be replaced with a newly conditioned key:

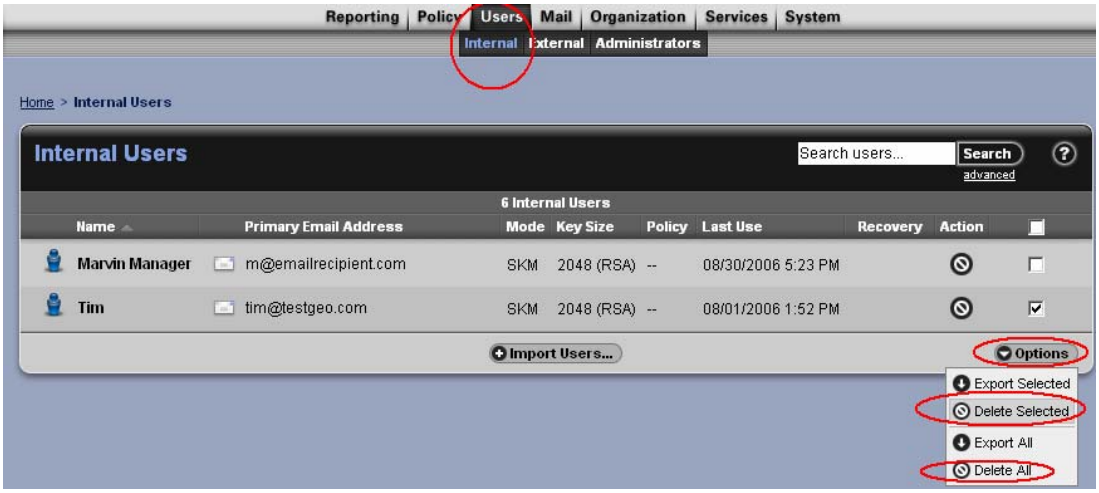


Figure B-11: Delete Internal Users – Step 1

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Clear the cache of PGP Universal Server to prevent associating old key attributes to new messages. Access the “Key Cache” screen, as shown in Figure B-12. Clear all cached keys.

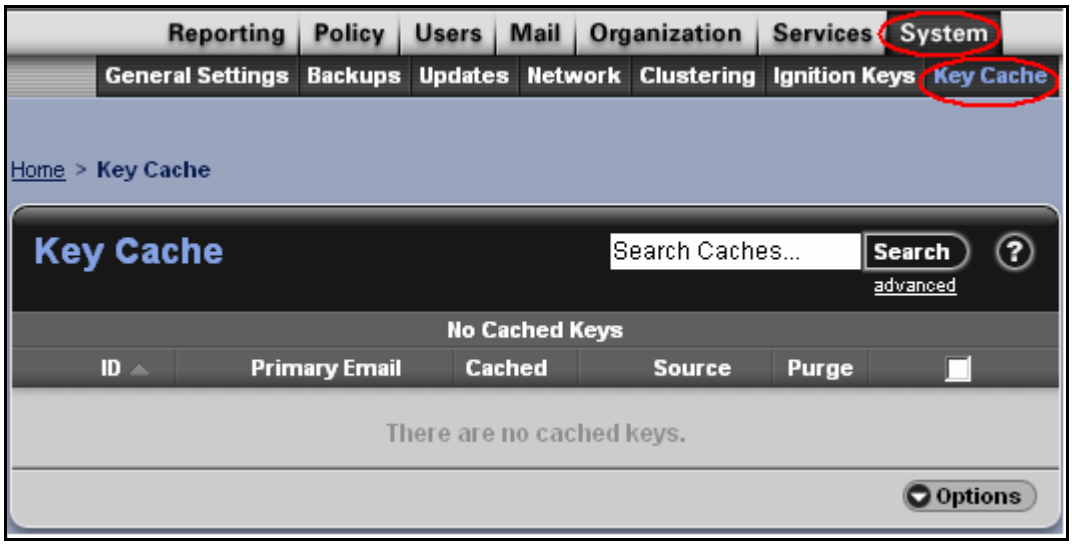


Figure B-12: Delete Internal Users – Step 2

Import the newly conditioned users, as shown in Figure B-13:

Figure B-13: Import Internal Users – Step 1

Select the **pubring** file you saved earlier. You may receive a warning that the keys were only partially imported, as shown in Figure B-14. You can ignore this message.

Figure B-14: Import Internal Users – Step 2

© 2006 PGP Corporation. All Rights Reserved.
APPROVED FOR EXTERNAL DISTRIBUTION

Now, import the private keyring called **secring.pkr**. You may need to refresh the page. The icons should return to a solid blue man group, as shown in Figure B-15, indicating that the users are now SKM.

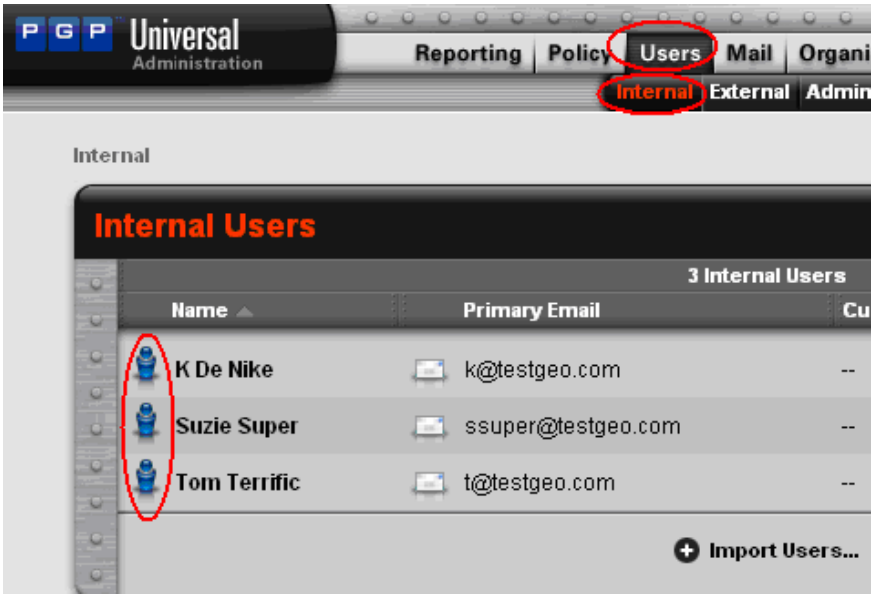


Figure B-15: Import Internal Users – Step 3

It is important to securely delete the private keyring file. If the same machine was used to perform all work, the keyring files should now be placed into the PGP Shredder.

This step completes the key conditioning operation.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

GKM and SCKM Key Conditioning

GKM and SCKM keys are secured by a passphrase known only to the holder of the private key. GKM keys are conditioned directly on the client, then exported and loaded into PGP Universal Server.

The user will enter the private passphrase that secures the keypair before it is conditioned, saved locally, and exported for eventual import into PGP Universal Server. With a single user in mind, follow the general technique for SKM Key Conditioning starting with the section entitled, “PGP Desktop Email: Remove Preferred Keyserver” on page 38.

© 2006 PGP Corporation. All Rights Reserved.

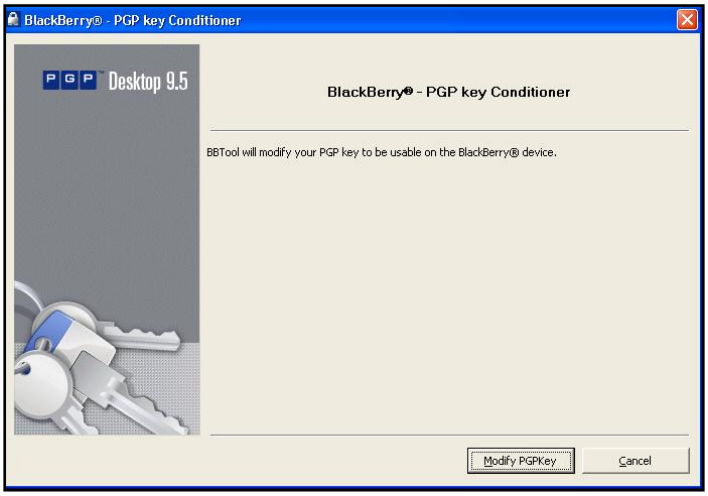
APPROVED FOR EXTERNAL DISTRIBUTION

Appendix C: Automated Key Conditioning

The BlackBerry Key Conditioning Preparation Tool (bbkeyprep) is an adjunct tool published by PGP Corporation for use with the PGP Support Package for BlackBerry. This tool is only supports keys created with PGP Desktop Email version 9.5.1 or greater. bbkeyprep automatically sets key attributes for CKM and GKM users. The attribute changes are described in Appendix B, beginning on page 36. The tool should be run by users who are responsible for the maintenance of their own keys. For bound users, bbkeyprep also publishes the updated key to PGP Universal Server.

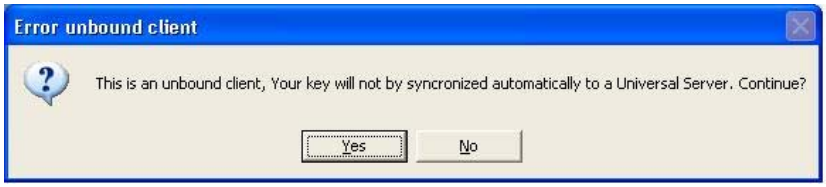
Step 1: Run bbkeyprep

Begin by executing bbkeyprep in the same directory as the DLL files that are provided with the tool. The introductory splash screen is presented:


BlackBerry® - PGP key Conditioner
PGP Desktop 9.5
BlackBerry® - PGP key Conditioner
BBTool will modify your PGP key to be usable on the BlackBerry® device.
Modify PGPKey
Cancel

Step 2: Bound Install?

If you are running an unbound copy of PGP Desktop Email (see page 4), you will see the warning at right, indicating that you must manually republish your key after running bbkeyprep.


Error unbound client
This is an unbound client, Your key will not by syncronized automatically to a Universal Server. Continue?
Yes
No

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

Step 3: Select Key

Select the key you wish to condition and enter the passphrase associated with the private key. If you have multiple keypairs on your keyring, you may select the pair you wish to condition by selecting the down arrow shown here.

Step 4: Republish

If your copy of PGP Desktop Email is bound to a PGP Universal Server, bbkeyprep will publish the new version of your key to PGP Universal Server. If you are using a stand-alone copy of PGP Universal Server, you must republish your key manually. Republishing is an essential step that permits your correspondents to view your BlackBerry compatible key properties.

How you republish your key depends upon how your correspondents expect to find your public key. See “Managing Public Keys” on page 22.

Troubleshooting

If you receive this error message, your private key is not stored locally. Your key attributes must be modified manually by the administrator of your PGP Universal Server.

© 2006 PGP Corporation. All Rights Reserved.

APPROVED FOR EXTERNAL DISTRIBUTION

PGP Corporation

3460 West Bayshore Road
Palo Alto, CA 94303 USA
Tel: +1 650 319 9000
Fax: +1 650 319 9001
Sales: +1 877 228 9747
Support: support.pgp.com
Website: www.pgp.com

© 2006 PGP Corporation

All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form by any means without the prior written approval of PGP Corporation.

The information described in this document may be protected by one or more U.S. patents, foreign patents, or pending applications.

PGP and the PGP logo are registered trademarks of PGP Corporation. RIM, Research In Motion, and BlackBerry are the registered trademarks of Research In Motion. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners.

The information in this document is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors.

All strategic and product statements in this document are subject to change at PGP Corporation's sole discretion, including the right to alter or cancel features, functionality, or release dates.

Changes to this document may be made at any time without notice.